

Министерство культуры Российской Федерации
ФГБОУ ВО «Кемеровский государственный институт культуры»
Факультет информационных и библиотечных технологий
Кафедра цифровых технологий и ресурсов

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки

42.04.05 Медиакоммуникации

Профиль подготовки

«Медиаменеджмент»

Квалификация (степень) выпускника

Магистр

Форма обучения

заочная

Утвержден на заседании кафедры
ЦТиР, 23.05.2022 г., протокол № 10

Составитель: Мишова В.В.

Кемерово

1. Перечень оцениваемых компетенций:

- ПК-3. Способен организовать работу и руководить предприятием (подразделением), осуществляющим медиакommunikационную деятельность.

2. Планируемые результаты обучения по дисциплине

Обучающийся должен демонстрировать следующие результаты обучения по дисциплине:

знать:

- компоненты концептуальной модели информационной безопасности; (31);
- классификацию и характеристику угроз информационной безопасности (32);
- классификацию преступлений в сфере информационной безопасности (33);
- нормативно-правовые документы в области защиты информации (34);
- требования к комплексной системе защиты информации (35).

уметь:

- выявлять угрозы информационной безопасности (У1);
- применять на практике нормативно-правовые документы в области защиты информации (У2);
- обосновывать и осуществлять выбор средств защиты информации (У3).

владеть:

- терминологией в сфере информационной безопасности (В1);
- способами предотвращения случайных и преднамеренных угроз информационной безопасности (В2).

3. Формируемые компетенции в структуре учебной дисциплины и средства их оценивания

№ п/п	Разделы (темы) дисциплины	Код оцениваемой компетенции	Планируемые результаты обучения по дисциплине (ЗУВ)	Оценочное средство
1	Раздел 1. Концептуальные положения защиты информации в информационных системах			
1.1	Информационная безопасность: определение понятия, состав, назначение	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы
1.2	Информационная система как объект защиты	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы
1.3	Угрозы информационной безопасности в информационных системах	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы
2	Раздел 2. Направления защиты информации в документационном обеспечении управления и архивном деле			
2.1	Правовое обеспечение информационной безопасности	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы

2.2	Организационное обеспечение информационной безопасности	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы
2.3	Программно-техническое обеспечение информационной безопасности	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	проверка результатов выполнения лабораторной работы, тестирование
2.4	Комплексная система защиты информации	ПК-3	31, 32, 33, 34, 35, У1, У2, У3, В1, В2	реализация учебного проекта

4. Оценочные средства по дисциплине для текущего контроля

4.1. Описание критериев оценивания компетенций на различных уровнях их формирования

При выставлении оценки преподаватель учитывает: логику, структуру, стиль ответа; культуру речи, манеру общения; готовность к дискуссии, аргументированность ответа; уровень самостоятельного мышления; умение приложить теорию к практике, решить задачи.

Нулевой уровень («неудовлетворительно»). Результаты обучения студента свидетельствуют:

З) об усвоении им некоторых элементарных знаний, но студент не владеет понятийным аппаратом изучаемой предметной области (учебной дисциплины);

У) не умеет установить связь теории с практикой;

В) не владеет способами решения практико-ориентированных задач.

Первый уровень - пороговый («удовлетворительно»). Достигнутый уровень оценки результатов обучения студента показывает:

З) знания имеют фрагментарный характер, отличаются поверхностностью и малой содержательностью; студент раскрывает содержание вопроса, но не глубоко, бессистемно, с некоторыми неточностями;

У) слабо, недостаточно аргументированно может обосновать связь теории с практикой;

В) способен понимать и интерпретировать основной теоретический материал по дисциплине.

Второй уровень повышенный («хорошо»). Студент на должном уровне:

З) раскрывает учебный материал: даёт содержательно полный ответ, требующий незначительных дополнений и уточнений, которые он может сделать самостоятельно после наводящих вопросов преподавателя;

У) демонстрирует учебные умения и навыки в области решения практико-ориентированных задач;

В) владеет способами анализа, сравнения, обобщения и обоснования выбора методов решения практико-ориентированных задач.

Третий уровень продвинутый («отлично»). Студент, достигающий должного уровня:

З) даёт полный, глубокий, выстроенный логично по содержанию вопроса ответ, используя различные источники информации, не требующий дополнений и уточнений;

У) доказательно иллюстрирует основные теоретические положения практическими примерами;

В) способен глубоко анализировать теоретический и практический материал, обобщать его, самостоятельно делать выводы, вести диалог и высказывать свою точку зрения.

4.2. Критерии оценивания для устного опроса

Знания, умения и навыки обучающихся при устном опросе определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

«Отлично» – обучающийся глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, не затрудняется с ответом при видоизменении задания, свободно справляется со сквозными вопросами, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.

«Хорошо» – обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения.

«Удовлетворительно» – обучающийся усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала.

«Неудовлетворительно» – обучающийся не знает значительной части программного материала, допускает существенные ошибки в изложении программного материала.

Шкала перевода баллов в оценки

Оценка	Минимальное количество баллов	Максимальное количество баллов
Отлично	41	50
Хорошо	31	40
Удовлетворительно	21	30
Неудовлетворительно	0	20

4.3. Лабораторные работы

В ходе освоения учебной дисциплины предусмотрено 3 лабораторных работ (6 часов). Описания лабораторных работ представлены в электронном учебно-методическом комплексе дисциплины, размещенном на сайте «Электронная образовательная среда КемГИК»).

Критерии оценивания:

- работа выполнена в полном объеме, даны правильные, развернутые ответы на контрольные вопросы - 5 баллов;
- работа выполнена в полном объеме, даны неточные или неполные ответы на контрольные вопросы - 4 балла;
- работа выполнена в полном объеме, даны неправильные ответы на контрольные вопросы - 3 балла;
- работа выполнена не в полном объеме, даны неточные или неполные ответы на контрольные вопросы - 2 балла;
- работа выполнена не в полном объеме, даны неправильные ответы на контрольные вопросы - 1 балл;
- работа не выполнена - 0 баллов.

4.4. Критерии оценивания учебных исследовательских проектов

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Защита проекта – публичное выступление, представляющее собой развернутое изложение исследованной проблемы. Продолжительность выступления – до 10 мин.

Выполняемые студентами проекты оцениваются по каждому из представленных критериев:

Тема проекта выбирается из списка, рекомендованного преподавателем; также возможен вариант самостоятельного выбора студентом темы, при условии обязательного согласования с преподавателем.

Выполняемые студентами проекты оцениваются по каждому из представленных

критериев:

Наименование критерия	Максимальное количество баллов
<i>Критерии оценки проекта</i>	
Соответствие содержания проекта заданной теме	2
Обоснованность результатов представленной работы	2
Грамотное использование цветового и шрифтового оформления	2
Качество представления графического материала, звуковой и видеoinформации	2
Гармоничность сочетания различных форм представления информации	2
Четкость и логичность выводов	2
Качество оформления отчета о выполненном проекте и презентации (отсутствие орфографических и синтаксических ошибок)	2
<i>Критерии оценки выступлений</i>	
Грамотность и логичность изложения материала	2
Глубина владения материалом	2
Аргументированность ответов на вопросы	2
	20

Каждый из критериев оценивается от 0 до 2 баллов, 1 – критерий выполнен частично, 2 – критерий выполнен в полном объеме. Таким образом, максимальное количество баллов за выполнение и защиту проекта составляет 20 баллов.

5. Оценочные средства по дисциплине для промежуточной аттестации и шкала оценивания

5.1. СПИСОК ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ И ПРОВЕРКИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Вопрос	Ответ
1. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА <i>Какие существуют основные уровни обеспечения защиты информации?</i> а) Законодательный б) Организационно-административный в) Программно-технический (аппаратный) г) Физический д) Вероятностный е) Распределительный	а) Законодательный б) Организационно-административный в) Программно-технический (аппаратный) г) Физический
2. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА <i>Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?</i> а) Доступность б) Целостность в) Конфиденциальность г) Управляемость д) Сложность	а) Доступность б) Целостность в) Конфиденциальность
3. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА	а) свойство системы, в которой

<p><i>Что такое доступность информации?</i></p> <p>а) Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия</p> <p>б) Свойство системы, обеспечивать беспрепятственный доступ к информации любых субъектов</p> <p>в) Свойство системы, обеспечивать закрытый доступ к информации любых субъектов</p> <p>г) Свойство информации, заключающееся в легкости ее несанкционированного получения и дальнейшего распространения (несанкционированного копирования)</p>	<p>циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия</p>
<p>4. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое целостность информации?</i></p> <p>а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p> <p>б) Свойство информации, заключающееся в возможности ее изменения любым субъектом</p> <p>в) Свойство информации, заключающееся в возможности изменения только единственным пользователем</p> <p>г) Свойство информации, заключающееся в ее существовании в виде единого набора файлов</p>	<p>а) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p>
<p>5. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое конфиденциальность информации?</i></p> <p>а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней</p> <p>б) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)</p> <p>в) Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора</p> <p>г) Свойство информации, заключающееся в ее</p>	<p>а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней</p>

<p>шифрования</p> <p>д) Свойство информации, заключающееся в ее принадлежности к определенному набору</p>	
<p>6. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что относится к угрозам информационной безопасности?</i></p> <p>а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию</p> <p>б) Классификация информации</p> <p>в) Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.)</p> <p>г) Сбои и отказы оборудования (технических средств) АС</p> <p>д) Ошибки эксплуатации (пользователей, операторов и другого персонала)</p> <p>е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)</p> <p>ж) Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)</p> <p>з) Иерархическое расположение данных</p>	<p>а) Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию</p> <p>в) Стихийные бедствия и аварии (наводнение, ураган, землетрясение, пожар и т.п.)</p> <p>г) Сбои и отказы оборудования (технических средств) АС</p> <p>д) Ошибки эксплуатации (пользователей, операторов и другого персонала)</p> <p>е) Преднамеренные действия нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов)</p> <p>ж) Последствия ошибок проектирования и разработки компонентов АС (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.)</p>
<p>7. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Какое определение информации дано в Законе РФ "Об информации, информатизации и защите информации"?</i></p> <p>а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления</p> <p>б) Получение сведений из глобальной информационной сети</p> <p>в) Систематизированные данные об экономике</p> <p>г) Это результаты компьютерных решений определенных задач</p>	<p>а) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления</p>
<p>8. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что относится к правовым мерам защиты информации?</i></p> <p>а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения</p> <p>б) Действия правоохранительных органов для защиты информационных ресурсов</p>	<p>а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения</p>

<p>в) Организационно-административные меры для защиты информационных ресурсов</p> <p>г) Действия администраторов сети защиты информационных ресурсов</p>	
<p>9. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Какие правовые документы решают вопросы информационной безопасности?</i></p> <p>а) Уголовный кодекс РФ</p> <p>б) Конституция РФ</p> <p>в) Закон "Об информации, информатизации и защите информации"</p> <p>г) Закон РФ "О государственной тайне"</p> <p>д) Закон РФ "О коммерческой тайне"</p> <p>е) Закон РФ "О лицензировании отдельных видов деятельности"</p> <p>ж) Закон РФ "Об образовании"</p> <p>з) Закон РФ "Об электронной цифровой подписи"</p>	<p>а) Уголовный кодекс РФ</p> <p>б) Конституция РФ</p> <p>в) Закон "Об информации, информатизации и защите информации"</p> <p>г) Закон РФ "О государственной тайне"</p> <p>д) Закон РФ "О коммерческой тайне"</p> <p>е) Закон РФ "О лицензировании отдельных видов деятельности"</p> <p>з) Закон РФ "Об электронной цифровой подписи"</p>
<p>10. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое государственная тайна?</i></p> <p>а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ</p> <p>б) Сведения о состоянии окружающей среды</p> <p>в) Все сведения, которые хранятся в государственных базах данных</p> <p>г) Сведения о состоянии здоровья президента РФ</p> <p>д) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне</p>	<p>а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ</p> <p>д) Конкретные сведения, в отношении которых компетентные органы и их должностные лица приняли решение об их отнесении к государственной тайне</p>
<p>11. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое коммерческая тайна?</i></p> <p>а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам</p> <p>б) Информация, к которой нет доступа на законном основании</p> <p>в) Информации, обладатель которой принимает меры к охране ее конфиденциальности</p> <p>г) Информация, содержащая в учредительных документах</p> <p>д) Информация, содержащая в годовых</p>	<p>а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам</p> <p>б) Информация, к которой нет доступа на законном основании</p> <p>в) Информации, обладатель которой принимает меры к охране ее конфиденциальности</p>

отчетах, бухгалтерских балансах, формах государственных статистических отчетов	
<p>12. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Согласно Федеральному закону «Об информации, информационных технологиях и защите информации» (№ 149-ФЗ от 27.07.2006 г.) не может быть ограничен доступ к:</i></p> <ul style="list-style-type: none"> а) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления; б) информации о состоянии окружающей среды; в) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных, составляющих государственную или служебную тайну; г) информации, накапливаемой в закрытых фондах в государственных, муниципальных и иных информационных системах. 	<p>а) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;</p> <p>б) информации о состоянии окружающей среды;</p>
<p>13. ДОПОЛНИТЬ ФРАЗУ</p> <p>Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами – это</p>	владелец информации
<p>14. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p>Комплекс мероприятий, направленных на обеспечение информационной безопасности – это _____ информации.;</p>	защита
<p>15. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое политика информационной безопасности организации</i></p> <ul style="list-style-type: none"> а) Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию б) Уничтожение, модификация, копирование информации в организации в) Набор административных документов, утвержденных в организации г) Совокупность механизмов компьютерных систем д) Инструкции администраторам по настройке информационных систем 	а) Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию
16. ВЫБРАТЬ ВАРИАНТЫ ПРАВИЛЬНОГО	а) Физическое управление

<p>ОТВЕТА</p> <p><i>Что относится к основным способам физической защиты?</i></p> <p>а) Физическое управление доступом б) Противопожарные меры в) Защита поддерживающей инфраструктуры г) Защита от перехвата данных д) Защита мобильных систем е) Проведение производственной зарядки ж) Проведение соревнований по профессиональному мастерству</p>	<p>доступом</p> <p>б) Противопожарные меры в) Защита поддерживающей инфраструктуры г) Защита от перехвата данных д) Защита мобильных систем</p>
<p>17. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Что такое несанкционированный доступ (нсд)?</i></p> <p>а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа б) Создание резервных копий в организации в) Правила и положения, выработанные в организации для обхода парольной защиты г) Вход в систему без согласования с руководителем организации д) Удаление не нужной информации</p>	<p>а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа</p>
<p>18. ДОПОЛНИТЬ ФРАЗУ</p> <p><i>Что такое идентификация?</i></p> <p>Процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации – это</p>	<p>идентификация</p>
<p>19. ДОПОЛНИТЬ ФРАЗУ</p> <p>Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа) – это</p>	<p>аутентификация</p>
<p>20. ВЫБРАТЬ ВАРИАНТ ПРАВИЛЬНОГО ОТВЕТА</p> <p><i>Какими способами обеспечиваются основные уровни антивирусной защиты?</i></p> <p>а) Поиск и уничтожение известных вирусов б) Поиск и уничтожение неизвестных вирусов в) Блокировка проявления вирусов г) Определения адреса отправителя вирусов д) Выявление создателей вирусов</p>	<p>а) Поиск и уничтожение известных вирусов б) Поиск и уничтожение неизвестных вирусов в) Блокировка проявления вирусов</p>

Тестирование обучающихся проводится после изучения дисциплины в соответствии с настоящей программой и является обязательным для всех студентов. Тесты включены в учебно-методический комплекс дисциплины, размещенный в «Электронной образовательной среде КемГИК».

Тесты включают 20 тестовых заданий. Результаты тестирования оцениваются в баллах в соответствии со следующими критериями:

- 100 – 90% (20– 19 правильных ответов) – 20 – 19 баллов, «отлично»;
- 89 – 75% (18 – 15 правильных ответов) – 18 – 15 баллов, «хорошо»;
- 74 – 60% (14 – 12 правильных ответов) – 14 – 12 баллов, «удовлетворительно»;

- ниже 60% (11 и менее правильных ответов) – 11 и менее баллов, «неудовлетворительно».

5.2 Методика и критерии оценки результатов обучения по дисциплине

Зачет по дисциплине принимается в форме собеседования (по вопросам), в ходе которого определяется уровень усвоения обучающимися материала, предусмотренного рабочей программой дисциплины.

Общие правила оценки успеваемости обучающегося в течение семестра

<i>Виды работ</i>	<i>Количество баллов</i>
Устный опрос	Максимум $5 \times 5 = 50$ баллов
Подготовка и защита творческого проекта	Максимум $20 \times 1 = 20$ баллов
Выполнение практических работ	Максимум $5 \times 3 = 15$ баллов
Тестирование	Максимум 15 баллов
<i>Итого за семестр:</i>	Максимум – 100 баллов

Критерии оценивания

Знания, умения и навыки обучающихся при промежуточной аттестации **в форме зачета** определяются «зачтено», «не зачтено».

«Зачтено» **выставляется, если обучающийся достиг уровней формирования компетенций: продвинутый, повышенный, пороговый** - обучающийся знает курс на уровне лекционного материала, базового учебника, дополнительной учебной, научной и методологической литературы, умеет привести разные точки зрения по излагаемому вопросу.

«Не зачтено» **соответствует нулевому уровню формирования компетенций;** обучающийся имеет пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой заданий.

При использовании 100-балльной шкалы оценивания при промежуточной аттестации, знания, умения и навыки обучающихся определяются в данной шкале и переводятся в оценки «зачтено», «не зачтено».

Шкала перевода баллов в оценки при промежуточной аттестации в форме зачета

Уровень формирования компетенции	Оценка	Минимальное количество баллов	Максимальное количество баллов
Продвинутый, повышенный, пороговый	Зачтено	60	100
Нулевой	Не зачтено	0	59